

NetIQ Access Manager

Op deze pagina vind je hoe je jouw Identity Provider-systeem kunt koppelen aan SURFconext als je gebruik maakt van de NetIQ Access Manager. Het volgende komt hier aan bod:

- **Stappenplan**
 - 1. User Store toevoegen
 - 2. SURFconext toevoegen aan de Identity Provider
 - 3. Voeg het token signing certificate van SURFconext toe
 - 4. Metadata URL doorgeven aan SURFnet
 - 5. Maak een attributen set aan
 - 6. Test de configuratie
- Compatibiliteits problemen met diensten

Stappenplan

Als je jouw Identity Provider-systeem wilt koppelen met NetIQ Access Manager, moet je de volgende stappen doorlopen:

1. Configureer een directory (User Store genoemd) in je Identity Provider-systeem. Deze is nodig voor de identiteiten waarmee je kunt inloggen op SURFconext-diensten.
2. Koppel SURFconext als SAML2.0 Service Provider aan je Identity Provider-systeem (hiermee configureer je jouw systeem ook als Identity Provider). In feite voeg je hierbij de SAML 2.0 metadata van SURFconext toe aan de NetIQ Identity Provider-configuratie.
3. Voeg het SURFconext-'token signing certificate' toe aan de 'Trusted Roots' van NetIQ Access Manager. Met deze certificaten worden straks SAML 2.0 berichten ondertekend, zodat we zeker weten ze van SURFconext komen en onderweg niet gewijzigd zijn.
4. Geef de metadata-URL van jouw Identity Provider-systeem door aan het SURFconext-team. Het SURFconext-team zorgt ervoor dat de URL wordt opgenomen in de SURFconext-configuratie.
5. Maak een attribute set en mapping aan voor de attributen die je moet meesturen naar SURFconext.
6. Test de configuratie.

In de tekst hierna wordt per stap uitgelegd, welke acties je moet uitvoeren om bovengenoemde stappen succesvol te doorlopen.

1. User Store toevoegen

Om een User Store-directory te configureren, moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.
2. Klik in de tab 'Local' onder 'User Stores' op 'New'. Je ziet dan onderstaand scherm:

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

m7

Name: *

Admin name: *
(Ex: cn=admin,o=novell)

Admin password: *

Confirm password: *

Directory type: ▾

☐ Install NMAS SAML method

☐ Enable Secret Store lock checking

LDAP timeout settings

LDAP Operation: ▾ seconds

Idle Connection: ▾ seconds

Server replicas

New | Delete | Validate 1 Item(s)

☐ Name	IP Address	Port	Use SSL	Max. Connections	Validation Status
☐ m7-directory	192.168.168.12	636	✓	20	✓

Search Contexts

New | Delete | ↑ | ↓ 1 Item(s)

☐ Context	Scope
☐ o=m7	One Level

<< Back | Finish | Cancel

3. Vul de juiste gegevens in (in ons geval een eDirectory-server van de organisatie 'm7') en klik op 'Finish'.

Merk op dat we een eDirectory replica en een search context (de plek in de directory information tree waaronder iedereen zich bevindt die SURFconext moet kunnen gebruiken; hier kunnen er meerdere van worden opgegeven) hebben gedefinieerd.

4. Update de configuratie onder 'Devices' -> 'Identity Servers' (zie de onderstaande afbeelding). Deze actie onderbreekt de services van Access Manager niet.

Access Manager | Devices | Policies | Auditing

Identity Servers

Notice: Warning

Any changes to 'IDP-Cluster' will not take effect until the servers using this configuration are updated.

Servers | Shared Settings

Start | Stop | Refresh | Actions 1 Item(s)

☐ Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration
IDP-Cluster	Update All ▾	✓	0		View		Edit Delete
192.168.168.12	Update ▾	✓	0	Complete	View	Linux	

Update [X]

☒ All Configuration (possible service interruption)
- Configuration changed

☐ Logging Settings

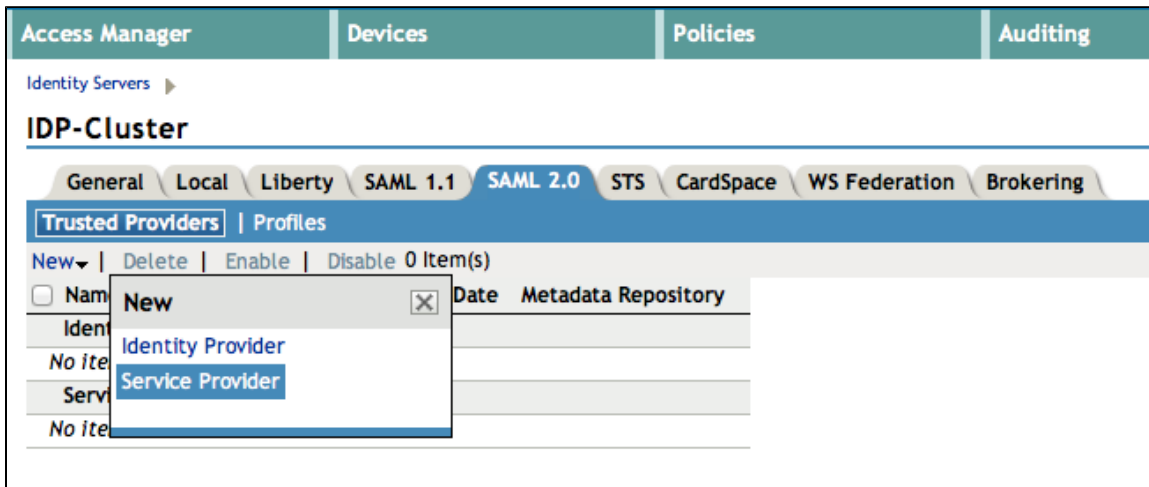
☐ Policy Settings

OK | Cancel

2. SURFconext toevoegen aan de Identity Provider

Om SURFconext toe te voegen aan je Identity Provider-systeem moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.
2. Zet in de tab 'General' onder 'Configuration' onderaan het vinkje bij SAML 2.0 aan.
3. Ga naar de tab 'SAML 2.0'. Kies nu 'New' en dan 'Service Provider' (zie onderstaande figuur).

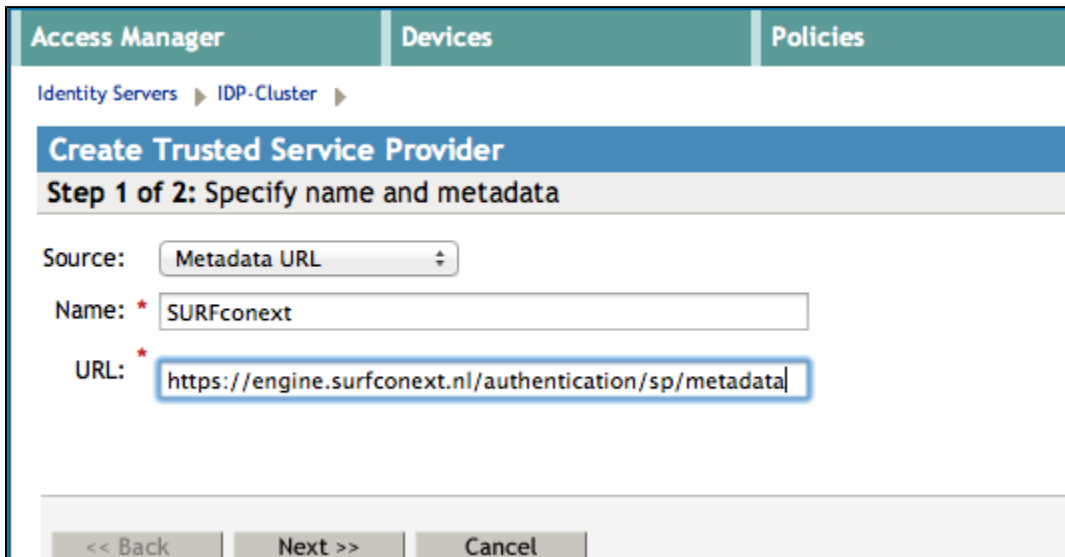


4. Vul de metadata-URL in, zoals je ziet in onderstaande afbeelding. De metadata-URL is:

- voor het koppelen aan SURFconext productie: <https://metadata.surfconext.nl/sp-metadata.xml>
- voor het koppelen aan SURFconext test: <https://metadata.test.surfconext.nl/sp-metadata.xml>

(de schermafbeelding hieronder vermeldt nog de oude url - gebruik die niet meer). Je voegt hiermee SURFconext toe als Service Provider.

Controleer de URL eerst in een browser en controleer ook het SSL-certificaat bij de URL (de browser geeft dit aan als je op het slotje klikt). Dit is belangrijk omdat je in een later stadium de metadata van SURFconext gaat gebruiken om een trustrelatie met SURFconext op te zetten.



5. Klik op 'Next'. Je ziet dan het volgende:

Access Manager | Devices | Policies | Auditing | Sec

Identity Servers ▸ IDP-Cluster ▸

Create Trusted Service Provider

Step 2 of 2: Confirm certificates

Signing Certificate

Subject: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL
 Validity: 24 januari 2011 - 23 januari 2021
 Issuer DN: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL
 Algorithm: SHA1withRSA
 Serial Number: cce2c6d5cc507d4d

<< Back | Finish | Cancel

6. Neem contact op met SURFnet als deze stap mislukt. Als het is gelukt, klik dan op 'Finish'. Je ziet dan het volgende scherm:

Access Manager | Devices | Policies | Auditing

Identity Servers ▸

IDP-Cluster

General | Local | Liberty | SAML 1.1 | SAML 2.0 | STS | CardSpace | WS Federation | Brokering

Trusted Providers | Profiles

New ▾ | Delete | Enable | Disable 1 Item(s)

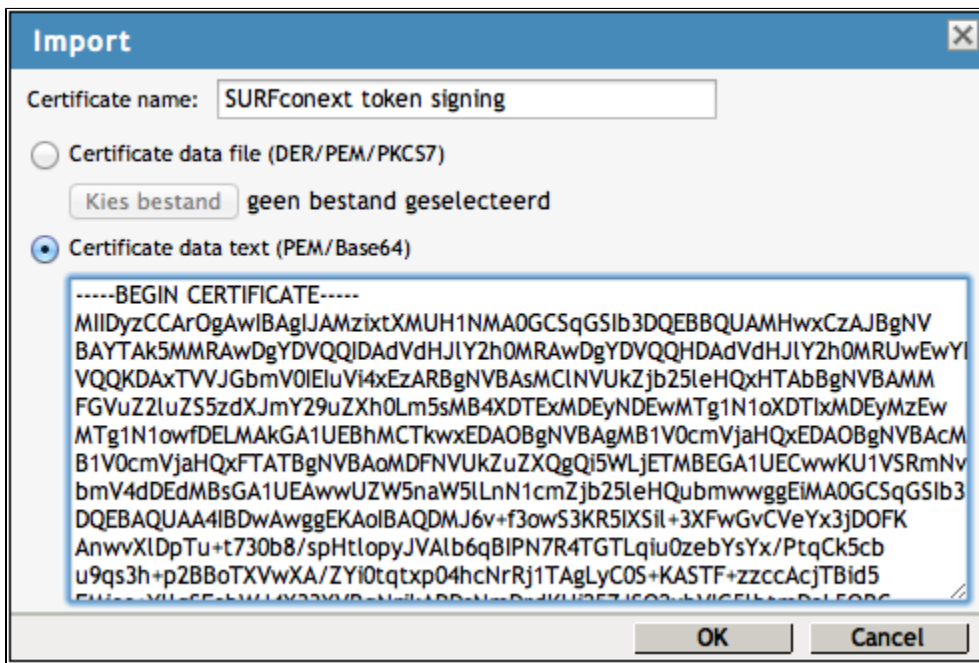
☐	Name	Enabled	Metadata Expiration Date	Metadata Repository
Identity Providers				
No items				
Service Providers				
☐	SURFconext	✓	Not specified	Not Applicable

7. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'.

3. Voeg het token signing certificate van SURFconext toe

SURFnet gebruikt bij SURFconext zogenaamde self signed tokencertificaten voor het ondertekenen van de SAML 2.0-berichten. Self signed tokencertificaten bieden voldoende garantie omdat SURFconext geen publieke dienst is.

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.
2. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte Service Provider.
3. Klik op de tab 'Metadata' en zoek het signing certificate (zie de figuur hieronder).
4. Selecteer en kopieer het signing certificaat zoals dat is gedaan in onderstaand figuur.



Geef het certificaat een beschrijvende naam (hier dus 'SURFconext token signing') en selecteer 'Certificate data text'. Plak hierin het gekopieerde certificaat.

6. Voeg in de regel boven het certificaat '-----BEGIN CERTIFICATE-----' toe en in de regel onder het certificaat '-----END CERTIFICATE-----' (dit is niet te zien in de afbeelding hierboven). Hiermee creëer je een geldig PEM-certificaat, zoals NetIQ Access Manager het graag ziet.

7. Klik op 'OK'. Als alles goed is gegaan, zie je het onderstaande scherm:

Access Manager	Devices	Policies	Auditing	Security
Certificates				
Certificates Trusted Roots External Trusted Roots Command Status				
Import... Delete Auto-Import From Server...				
Name		Subject	Starting Date	Ending Date
☐ configCA		O=netiqam_tree, OU=Organizational CA	12 november 2012	4 februari 2036
☒ SURFconext_token_signing		CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL	24 januari 2011	23 januari 2021

4. Metadata URL doorgeven aan SURFnet

1. Controleer of op de volgende URL <https://<servernaam>/nidp/saml2/metadata> geldige XML laat zien. Deze metadata bevat alle informatie die nodig is om jouw organisatie aan SURFconext toe te voegen.

Deze URL moet ook voor SURFnet benaderbaar zijn.

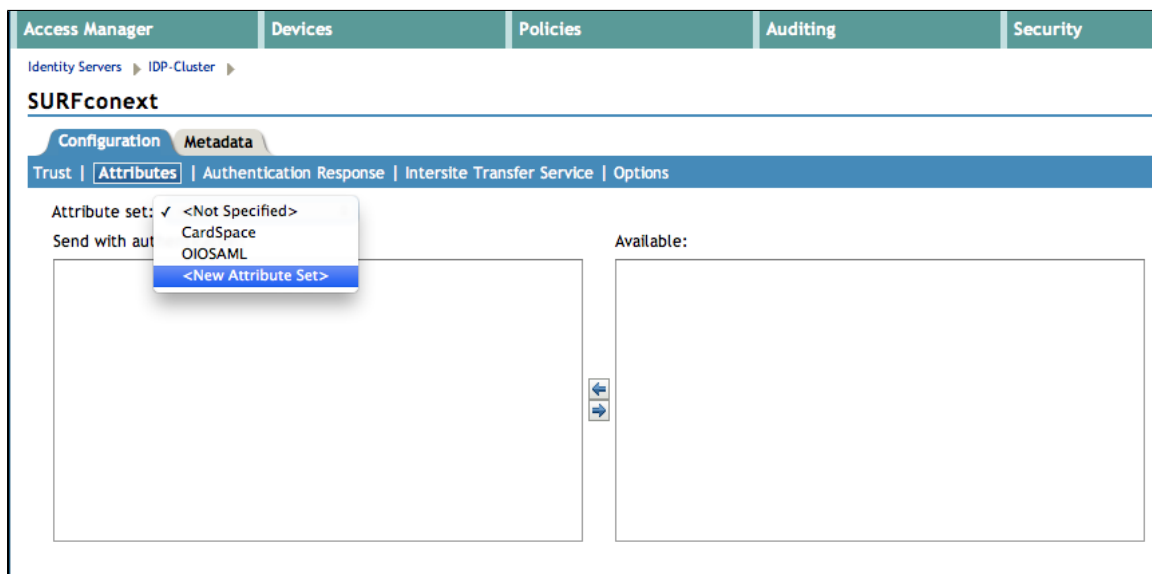
2. Geef deze URL door aan het SURFconext-team (support@surfconext.nl) en wacht op bericht waarin het SURFconext-team aangeeft dat de metadata is geconfigureerd. Je kunt intussen wel verder met de overige stappen, behalve de laatste controle.

5. Maak een attributen set aan

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.

2. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte Service Provider.

3. Klik in de tab 'Configuration' op 'attributes' en kies bij het uitrolmenu 'attribute set' voor '<New Attribute Set>'. Zie hieronder in de figuur:



4. Geef de nieuwe attributenset een naam, zoals in onderstaand figuur.

Klik op 'Next' en vervolgens in het volgende scherm op 'New'.

Voor SURFconext zijn conform [Vereiste attributen](#) volgende attributen verplicht:

```
urn:mace:dir:attribute-def:mail
urn:mace:dir:attribute-def:displayName
urn:mace:dir:attribute-def:cn
urn:mace:dir:attribute-def:sn
urn:mace:dir:attribute-def:givenName
urn:mace:terena.org:attribute-def:schacHomeOrganization
urn:mace:dir:attribute-def:uid
urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:mace:dir:attribute-def:eduPersonAffiliation
urn:mace:dir:attribute-def:eduPersonScopedAffiliation
```

De betekenis van deze attributen is te vinden op de attributenschema pagina van SURFconext. Zie [Attributen in SURFconext \(NL\)](#).

5. Kies in het scherm hieronder voor de local attribute-waarde. Let erop dat je voor de meeste attributen een naam moet kiezen die in LDAP voorkomt (aangegeven met 'LDAP Attribute'). Vul voor 'remote attribute' de volledige urn in zoals gespecificeerd in het [attributenschema](#) van SURFconext.

Add Attribute Mapping

Local attribute:

Ldap Attribute:mail [LDAP Attribute Profile]

Constant:

Remote attribute:

urn:mace:dir:attribute-def:mail (optional)

Remote namespace:

none

Remote format:

unspecified

OK

Cancel

6. Klik op 'OK' en herhaal dit voor de overige attributen.

Kies de attributen mapping zorgvuldig en correct. Je moet dus het locale attribuut bij urn:mace:dir:attribute-def:mail voor iedereen daadwerkelijk wijzen in een geldig e-mailadres.

Voor schacHomeOrganization moet je een 'Constant' kiezen met als waarde de domeinnaam van de Identity Provider. In ons geval 'm-7.nl'.

Bij een standaardinstallatie van eDirectory die wordt gebruikt als User Store wordt meestal niet 'uid' gebruikt als inlognaam maar 'cn'. Map daarom het LDAP-attribuut 'cn' op urn:mace:dir:attribute-def:uid.

Het resultaat hiervan zie je in onderstaand figuur.

Access Manager	Devices	Policies	Auditing
Identity Servers > IDP-Cluster > SURFconext >			
Create Attribute Set			
Step 2 of 2: Define attributes			
New Delete 6 Item(s)			
☐ Local Attribute	maps to	Remote Attribute	
☐ Ldap Attribute:mail [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:mail	
☐ Ldap Attribute:cn [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:uid	
☐ Constant Value: m-7.nl	<-->	urn:mace:terena.org:attribute-def:schacHomeOrganization	
☐ Ldap Attribute:displayName [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:displayName	
☐ Ldap Attribute:sn [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:sn	
☐ Ldap Attribute:givenName [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:givenName	

7. Klik op 'Next'. Je kunt kiezen welke attributen uit de set je wilt gebruiken. Zie de figuur hieronder:

In bovenstaand voorbeeld moeten alle attributen links komen te staan (bij 'Send with authentication').

8. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'. Vergeet deze stap niet!

6. Test de configuratie

Nadat je van SURFnet bevestiging hebt ontvangen dat jouw metadata is toegevoegd, kun je jouw nieuwe Identity Provider-systeem testen op een test-Service Provider. Hiervoor heeft SURFnet de volgende URLs beschikbaar: <https://engine.surfconext.nl/authentication/sp/debug> en <https://profile.surfconext.nl/>.

Je hebt een testkoppeling zolang je de bijlage bij het SURFnet-contract voor SURFconext nog niet ondertekend heb teruggestuurd naar SURFnet. Daarna heb je automatisch een productiekoppeling. Overigens zijn de URL's misschien aan verandering onderhevig. Deze moet je nog wel eerst bij SURFnet verifiëren.

Compatibiliteits problemen met diensten

Het is bekend dat er compatibiliteitsproblemen zijn tussen NetIQ Access Manager en Service Providers die Microsoft (.NET) gebruiken. Deze problemen worden veroorzaakt door het anders interpreteren van de SAML2.0 specificatie. Volgens Microsoft kan een URI alleen een absolute URI (zie [wikipedia](https://en.wikipedia.org/wiki/URI) voor uitleg over URIs) zijn, terwijl NetIQ Access Manager ook gebruik maakt van URI verwijzingen (zoals ook mogelijk is volgens de SAML2.0 en XSD specificatie). Om deze problemen voor te zijn moet je het authenticatie contract van de NetIQ Access Manager Identity Provider aanpassen.

Als je het authenticatie contract wilt aanpassen om URI-verwijzingen te veranderen naar absolute URI's, dan moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'. Ga vervolgens naar de tab 'Local' en klik onder 'Contracts' op 'new' (zie onderstaand figuur).

Access Manager | Devices | Policies | Auditing | Security

Identity Servers >

IDP-Cluster ?

General | Local | Liberty | SAML 1.1 | SAML 2.0 | STS | CardSpace | WS Federation | Brokering

User Stores | Classes | Methods | **Contracts** | Defaults

New | Delete 4 Item(s)

☐ Name	URI	Level
☐ Name/Password - Basic	basic/name/password/uri	0
☐ Name/Password - Form	name/password/uri	0
☐ Secure Name/Password - Basic	secure/basic/name/password/uri	0
☐ Secure Name/Password - Form	secure/name/password/uri	0

OK Cancel Apply

2. Vul de gegevens in zoals in het onderstaand figuur:

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

Create Authentication Contract ?

Step 1 of 2: Configuration

Display name:

URI:

Password expiration servlet:

☐ Allow user interaction

Authentication Level:

Authentication Timeout: Minutes

Activity Realm(s):

☐ Satisfiable by a contract of equal or higher level

☐ Satisfiable by External Provider

Requested By:

Allowable Class:

If you add more than one X509 method, only the first one will be used and it will automatically be moved to the top of the list.

Methods:

Available methods:

- ☐ Name/Password - Basic
- ☐ Secure Name/Password - Basic
- ☐ Secure Name/Password - Form

< >

<< Back Next >> Cancel

Vergeet niet de Method 'Name/Password - Form' aan te klikken en vervolgens op de  te klikken!

3. Klik op 'Next'.

4. Vul bij Text in: Name/Password - Form URI en selecteer bij Image: Form Auth Username Password (zie onderstaand figuur).

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

Create Trusted Identity Provider ?

Step 2 of 2: Enter authentication card values

ID:

Text:

Image: 

☒ Show Card

☐ Passive Authentication Only

<< Back Finish Cancel

5. Klik op 'Finish'.

6. Stel nu deze nieuwe Authenticatie Contract in als de Default Authenticatie Contract. Dit doe je door naar het tabblad 'Defaults' te gaan. Vervolgens selecteer je bij Authentication Contract de nieuwe 'Name/Password - Form URI' contract (zie onderstaand figuur).

Access Manager | Devices | Policies | Auditing | Security

Identity Servers >

IDP-Cluster ?

General Local Liberty SAML 1.1 SAML 2.0 STS CardSpace WS Federation Brokering

User Stores | Classes | Methods | Contracts | **Defaults**

Defaults

User Store:

Authentication Contract:

Authentication Type	Default Contract
Name Password:	<None>
Secure Name Password:	<None>
X509:	<None>
Smart Card:	<None>
Smart Card PKI:	<None>
Token:	<None>

OK Cancel Apply

7. Klik op 'OK'.

8. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'. Vergeet deze stap niet!